

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

STONEX GROUP INC. and STONEX
FINANCIAL INC.,

Plaintiffs,

- against -

HOWARD SHIPMAN,

Defendant.

Case No. _____

**DECLARATION OF MICHAEL WAREMAN IN SUPPORT OF PLAINTIFFS'
MOTION FOR A TEMPORARY RESTRAINING ORDER**

I, Michael Wareman, hereby declare as follows,

1. I am Associate Director of Cyber Security for Plaintiffs StoneX Group Inc. and StoneX Financial Inc. (collectively "StoneX" or the "Company"). I have personal knowledge of the facts set forth herein and, if called to do so, could competently testify thereto.

2. I have worked at StoneX since August 3, 2020 and have served in my current role since that date. I report to Abbey Perkins, Chief Information Officer.

3. Because of the highly confidential and valuable nature of StoneX's business information, and in accordance with the compliance obligations imposed on StoneX by financial regulators in multiple jurisdictions across the globe, the Company utilizes many different layers and forms of information security.

4. Upon starting any company-owned StoneX laptop, the laptop prompts the user with the following:

Attention – Please Read! This computer is for StoneX business use. In line with information security, policy, all system use, including e-mail, Internet, and intranet use may be monitored to guard against unauthorized or inappropriate use. Use of this system constitutes, consent to monitoring, in accordance with local laws. Unauthorized use may result in reprimand, financial penalties, and/or legal action.

The user must then accept this statement by clicking “ok” before logging in.

5. StoneX employees are required to follow StoneX’s Acceptable Use Policy (“AUP”) and Acceptable Use of IT Facilities Policy (“AUPF”). These policies are readily available to all StoneX employees on the corporate intranet. True and correct copies of StoneX’s AUP (Exhibit 1) and AUPF (Exhibit 2) are attached hereto.

6. The AUP details StoneX’s expectations regarding employee protection of StoneX’s data, information, systems, networks and computers. The AUP includes requirements to ensure information security, such as: (a) prohibiting unauthorized access to accounts (including stealing or misusing a password), programs and/or data, (b) requiring that StoneX’s proprietary information stored on electronic and computing devices whether owned or leased by StoneX, the employee or a third party, remains the sole property of StoneX, (c) requiring that data owned, processed or held by the Company, must be protected in accordance with data protection standards, and (d) disclosing that the Company may log all forms of employee IT use and communications, and that the Company reserves the right to monitor computer equipment, systems and network traffic.

7. Section 1.0 of the AUP provides that computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP remain the property of StoneX.

8. Section 3.5 of the AUP maintains that accessing data, a server or an account for any purposes other than conducting StoneX business is prohibited.

9. Section 3.8 of the AUPF provides StoneX’s Exit Procedures, which states:

Upon leaving the Company it is expected that users:

- Promptly return all Company IT equipment in reasonable working condition.
- Do not delete any data which belongs to the Company.
- Transfer any data which may be needed by the Company to an appropriate server or colleague prior to departure.
- Ensure any of their own data that they wish to keep is removed from the Company's systems, as they will not be entitled to access this once they leave.
- Review and conform to any other procedures set out by the Company in relation to departure.

10. In addition to Company policies, StoneX Group Inc. employs approximately 80 individuals globally to ensure the Company's cyber security. These employees operate via various teams, including Identity & Access Management, Cybersecurity/Security Operations, IT Governance, Risk & Compliance, Third Party Vendor Risk and Business Resiliency. All teams report to the Chief Information Officer.

11. StoneX also employs a stand-alone internal audit team, which exists outside of StoneX's cyber security group and reports directly to StoneX's executive committee. Among other things, this team conducts independent audits of StoneX's cyber security systems.

12. Further, StoneX performs regular third-party penetration testing to ensure the security of its network.

13. StoneX ensures employee desktops, laptops, mobile devices, servers, and databases are initially configured to meet the Company's cyber security requirements.

14. To log on to StoneX's network, employees can utilize a virtual private network ("VPN"), which is an online portal used to access StoneX's network, or connect directly from one of StoneX's physical offices using an authorized device. VPN login requires a username, password, multi-factor verification and an authorized StoneX device. Access to StoneX's network from within a StoneX office requires the use of a username, password and authorized StoneX device.

15. StoneX also uses best-in-class endpoint detection and response (“EDR”) tools to detect and investigate threats to its network. It also utilizes malware and virus detection/prevention tools, and works with third-party providers, such as Microsoft and CrowdStrike, to further monitor and protect its network.

16. Across its entire network, StoneX utilizes the ‘least privilege’ principle, which means that StoneX employees only have access to the data or information that they need to perform their job.

17. StoneX’s Confidential information is heavily guarded. In addition to all of the other security measures in place throughout StoneX’s network, the Company utilizes additional monitoring, vulnerability management and remediation programs to ensure the protection of this information.

18. Upon information and belief, Shipman was fully aware of StoneX’s cyber security policies and procedures.

19. Between September 2021 and March 2022 StoneX’s Cyber Security Architect Frank McGovern and Michael Glatz, Manager of Security Engineering, both of whom report to me, spent hours speaking directly with Shipman about the various rules and regulations of cyber security compliance that were applicable to him and his team, including sharing copies of policies applicable to the environment.

20. In addition, Vito Demonte, Associate Director of IT Governance Risk and Compliance, also shared ten separate StoneX’s policies about network management, password management, change management, privileged access management, audit, control, access control and encryption with Shipman.

21. Upon information and belief, Shipman used non-StoneX owned or approved computers, servers, and personal devices, such as his personal computer, a personally licensed Linode cloud server, and other non-StoneX devices to perform his responsibilities as an employee of StoneX.

22. The IP address – [REDACTED] – corresponds to a non-StoneX Linode cloud server, which upon information and belief, is Shipman’s personal cloud server (“Shipman’s IP Address”). This is evidenced through authentication logs utilizing a private key that only Shipman possessed.

```
{
  "status": "success",
  "continent": "North America",
  "continentCode": "NA",
  "country": "United States",
  "countryCode": "US",
  "region": "NJ",
  "regionName": "New Jersey",
  "city": "Cedar Knolls",
  "district": "",
  "zip": "07927",
  "lat": 40.8225,
  "lon": -74.4592,
  "timezone": "America/New_York",
  "offset": -18000,
  "currency": "USD",
  "isp": "Linode, LLC",
  "org": "Linode",
  "asn": "AS63949 Akamai Technologies, Inc.",
  "asname": "AKAMAI-AP",
  "mobile": false,
  "proxy": false,
  "hosting": true
}
```

1	corvo-004/vnc/sock/auth.log:118c	9 09:58:25	corvo-004	sshd(17223): pam_unix(sshd:session): session opened for user pianman by 49(40)	
2	corvo-004/vnc/sock/auth.log:118c	9 09:58:25	corvo-004	sshd(17223): New session 37801 of user pianman	
3	corvo-004/vnc/sock/auth.log:118c	9 09:58:30	corvo-004	sshd(17223): Accepted publickey for pianman from 69.164.211.49 port 41420 ssh2: RSA SHA256:Kino92d6FxxwXk3JdcNpYH10oFlw72T5c231Q	
4	corvo-004/vnc/sock/auth.log:118c	9 09:58:30	corvo-004	sshd(17223): pam_unix(sshd:session): session opened for user pianman by 49(40)	
5	corvo-004/vnc/sock/auth.log:118c	9 09:59:10	corvo-004	sshd(17223): New session 31162 of user pianman	
6	corvo-004/vnc/sock/auth.log:118c	9 10:01:33	corvo-004	sshd(17369): Accepted publickey for pianman from 69.164.211.49 port 41422 ssh2: RSA SHA256:Kino92d6FxxwXk3JdcNpYH10oFlw72T5c231Q	
7	corvo-004/vnc/sock/auth.log:118c	9 10:01:36	corvo-004	sshd(17369): pam_unix(sshd:session): session opened for user pianman by 49(40)	
8	corvo-004/vnc/sock/auth.log:118c	9 10:01:36	corvo-004	sshd(17369): New session 31765 of user pianman	
9	corvo-004/vnc/sock/auth.log:118c	9 10:01:58	corvo-004	sshd(17591): Disconnected from user pianman 69.164.211.49 port 41422	
10	corvo-004/vnc/sock/auth.log:118c	9 10:01:59	corvo-004	sshd(17591): pam_unix(sshd:session): session closed for user pianman	
11	corvo-004/vnc/sock/auth.log:118c	9 10:02:01	corvo-004	sshd(17916): Accepted publickey for pianman from 69.164.211.49 port 41424 ssh2: RSA SHA256:Kino92d6FxxwXk3JdcNpYH10oFlw72T5c231Q	
12	corvo-004/vnc/sock/auth.log:118c	9 10:02:01	corvo-004	sshd(17916): pam_unix(sshd:session): session opened for user pianman by 49(40)	
13	corvo-004/vnc/sock/auth.log:118c	9 10:02:01	corvo-004	sshd(17916): New session 31743 of user pianman	
14	corvo-004/vnc/sock/auth.log:118c	9 10:02:43	corvo-004	sshd(17937): Disconnected from user pianman 69.164.211.49 port 41424	
15	corvo-004/vnc/sock/auth.log:118c	9 10:02:43	corvo-004	sshd(17937): pam_unix(sshd:session): session closed for user pianman	
16	corvo-004/vnc/sock/auth.log:118c	9 10:31:17	corvo-004	sshd(17397): Accepted publickey for pianman from 69.164.211.49 port 41423 ssh2: RSA SHA256:Kino92d6FxxwXk3JdcNpYH10oFlw72T5c231Q	
17	corvo-004/vnc/sock/auth.log:118c	9 10:31:17	corvo-004	sshd(17397): pam_unix(sshd:session): session opened for user pianman by 49(40)	
18	corvo-004/vnc/sock/auth.log:118c	9 10:31:17	corvo-004	sshd(17397): New session 31194 of user pianman	
19	corvo-004/vnc/sock/auth.log:118c	9 10:42:34	corvo-004	sshd(17318): Disconnected from user pianman 69.164.211.49 port 41423	
20	corvo-004/vnc/sock/auth.log:118c	9 10:42:34	corvo-004	sshd(17318): pam_unix(sshd:session): session closed for user pianman	
21	corvo-004/vnc/sock/auth.log:118c	9 10:42:35	corvo-004	sshd(17491): Accepted publickey for pianman from 69.164.211.49 port 41430 ssh2: RSA SHA256:Kino92d6FxxwXk3JdcNpYH10oFlw72T5c231Q	
22	corvo-004/vnc/sock/auth.log:118c	9 10:42:35	corvo-004	sshd(17491): pam_unix(sshd:session): session opened for user pianman by 49(40)	
23	corvo-004/vnc/sock/auth.log:118c	9 10:42:35	corvo-004	sshd(17491): New session 31196 of user pianman	
24	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
25	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
26	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
27	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
28	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
29	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
30	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
31	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
32	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
33	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
34	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
35	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
36	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
37	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
38	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
39	corvo-004/vnc/sock/auth.log:118c	9 16:47:39	corvo-004	sshd(49354): pam_unix(sshd:session): session opened for user root by pianman(41460)	
40	corvo-004/vnc/sock/auth.log:				

23. StoneX's security team coordinated to terminate Shipman's access to its systems and network – before Shipman was notified of his termination. However, unbeknownst to StoneX, Shipman's pre-existing connection to the Pascal Azure servers from his Linode server allowed him to remain on the network.

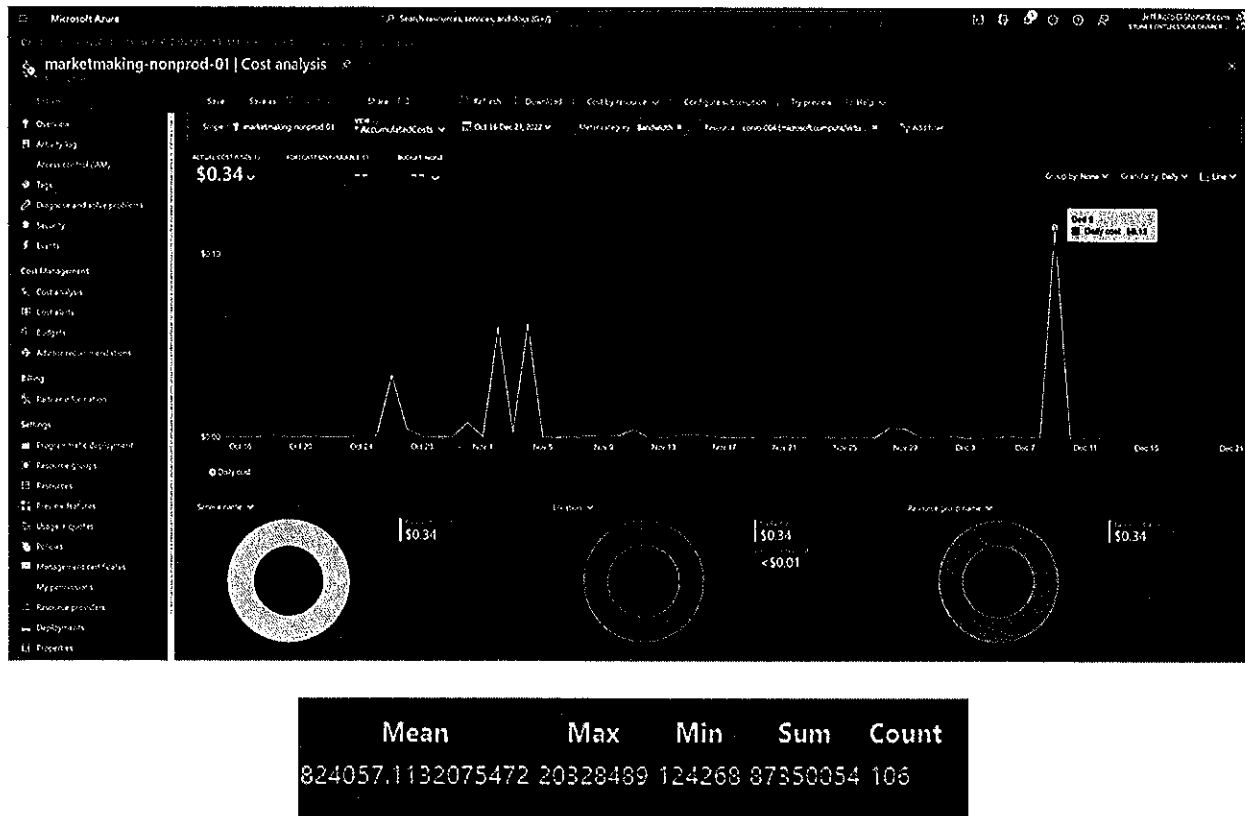
24. Specifically, on December 9, 2022, Shipman logged into the Pascal Azure servers from Shipman's IP Address (i.e. the Linode server), rather than his StoneX issued laptop, at roughly 8:58am CST. As discussed further below, Shipman remained logged into the Pascal Azure servers until 4:45pm CST that evening. A period that included nearly 75 minutes after he was terminated at 3:30pm CST.

25. Shipman – via his “pianoman” username – was the only individual logged into the Pascal Azure servers between 3:00pm and 4:45pm CST.

26. After termination, Shipman maintained his connection via Shipman's IP Address. Even though he was by this point an ex-StoneX employee with no authorized access to StoneX data, he continued not only to access that data, he manipulated and egressed StoneX's intellectual property.

27. Between 3:30pm and 4:45pm CST, Shipman deleted the server “bash history” from November 7, 2022 onwards. The “bash history” is a log of all prior coding commands utilized on a server that would reveal all of his actions. Without such history, StoneX is unable to determine if Shipman accessed the Pascal Azure server in the days leading up to his termination, or after his termination.

28. Independent logs from Microsoft, which Shipman was unable to delete, confirm that 87 MBs of data was egressed from the Pascal Azure servers during this period.



29. Following the egress of data, Shipman (logged in as “pianoman”) deleted his account’s server bash history from the Pascal Azure server named Corvo-004 at approximately 4:05pm CST.

30. Shortly after, Shipman switched from his “pianoman” personal account to the “root” account. Only Shipman, with his Administrator access, could have switched their account username from “pianoman” to “root.”

31. At 4:13pm CST, the administrator level “root” account, under Shipman’s control, deleted the bash history associated with any actions taken by it.

32. My security team was alerted to this activity as two security alerts were raised after Shipman’s termination for history files being cleared by the account “pianoman” and “root” at 4:05pm CST and 4:13pm CST.

Severity	Alert title	Affected resource	Resource Group	Activity start time (UTC-6)	Mitre ATT&CK tactics	Status
Medium	A history file has been cleared	corvo-004	PASCAL-N-TRA-FIN	12/09/22 04:13 PM	Defense Evasion	Active
Medium	A history file has been cleared	corvo-004	PASCAL-N-TRA-FIN	12/09/22 04:05 PM	Defense Evasion	Active

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Security alert

A history file has been cleared

Medium

Severity

Active

Status

12/09/22...

Activity time

Alert description

Copy alert JSON

Analysis of host data indicates that the command history log file has been cleared. Attackers may do this to cover their traces. The operation was performed by the specified user account.

Affected resource

corvo-004

Virtual machine

marketmaking-nonprod-01

Subscription

Alert details

Take action

General information

Compromised Host

CORVO-004

User Name

pianoman

Account Session ID

0x8488

Suspicious Process

/usr/bin/rm

Suspicious Command Line

rm -v .bash_history

Suspicious Process ID

0x7b0fa

Detected by

Microsoft

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Security alert

A history file has been cleared

Medium

Severity

Active

Status

12/09/22...

Activity time

Alert description

Copy alert JSON

Analysis of host data indicates that the command history log file has been cleared. Attackers may do this to cover their traces. The operation was performed by the specified user account.

Affected resource

corvo-004

Virtual machine

marketmaking-nonprod-01

Subscription

Alert details

Take action

General information

Compromised Host

CORVO-004

User Name

root

Account Session ID

0x848f

Suspicious Process

/usr/bin/rm

Suspicious Command Line

rm .bash_history

Suspicious Process ID

0x7da7e

Detected by

Microsoft

8

33. Additionally, after Shipman's termination at 3:30pm CST and final logoff of his login from his Linode server at approximately 4:45pm CST on December 9, 2022, Shipman made additional attempts to access StoneX's network that evening and throughout the weekend.

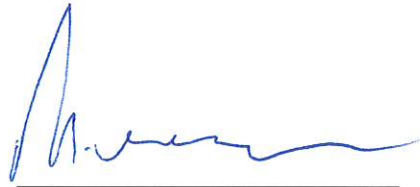
34. StoneX's outside counsel, Proskauer Rose, hired Charles River Associates ("CRA") on StoneX's behalf to perform forensic examinations of StoneX's computer systems, and Shipman's StoneX laptop. As I understand the work being performed by CRA, they are relying on tools and skills that we do not possess internally at StoneX.

35. CRA was retained on or about December 27, 2022. Due to the delay by Shipman in returning his StoneX laptop, CRA only received the laptop during the day on January 3, 2022.

36. To date, StoneX has spent more than \$5,000.00 in order to (a) respond to Shipman's conduct and (b) pay CRA to conduct its damage assessment of the data taken from Shipman's computer.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing statements are true and correct to the best of my knowledge.

Dated: Chicago, Illinois
January 18, 2023

A handwritten signature in blue ink, appearing to read 'Michael Wareman', written over a horizontal line.

Michael Wareman